AO 91 (Rev. 02/09) Criminal Complaint

United States District Court

for the
Western District of New York

United States of America

v.

Case No. 19-mj- 5167

DAVID MICHAEL CALAIACOVO

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about June 27, 2019, in the Western District of New York, the defendant, **David Michael Calaiacovo**, did knowingly possess material, that is, a Toshiba Satellite L645D laptop computer bearing serial number YA053651W, that contained images of child pornography, as defined in Title 18, United States Code, Section 2256(8), that had been transported in and affecting interstate and foreign commerce.

All in violation of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(b)(2).

This Criminal Complaint is based on these facts:

☒ Continued on the attached sheet.

Complainant's signature

JOHN A. KOSICH, JR.
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
Printed name and title

Sworn to before me and signed in my presence.

Date: July 2, 2019

Judge's signature

City and State: Buffalo, New York

MICHAEL J. ROEMER
UNITED STATES MAGISTRATE JUDGE
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, **John A. Kosich, Jr.** , being duly sworn, depose and state the following:

1. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to Buffalo, New York and have been so employed since January of 2007. As such, I am a law enforcement officer of the United States, within the meaning of Section 115(c)(1) of Title 18, United States Code, who is "authorized by law or by Government agency to engage in or supervise the prevention, detection, investigation or prosecution of any violation of Federal criminal law." Prior to my appointment as an HSI Special Agent I was employed as an Officer with United States Customs and Border Protection and as an Inspector with the former Immigration and Naturalization Service since June of 1998. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the receipt and possession of child pornography, in violation of Title 18, U.S.C., Section 2252A(a)(5)(B). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review multiple examples of child pornography (as defined in Title 18, U.S.C., § 2256) in various forms of media including computer media. I have also participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses.

2. I make this affidavit in support of a criminal complaint charging **David Michael CALAIACOVO (hereinafter CALAIACOVO)** with violations of Title 18, United States Code, Section 2252 2252A(a)(2)(A) [Receipt of Child Pornography], and 2252A(a)(5)(B) [Possession of Child Pornography].

3. The statements contained in this affidavit are based upon my investigation, information provided to me by other law enforcement personnel, and on my experience and training as a Special Agent of HSI. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that CALAIACOVO knowingly violated Title 18, United States Code, Section 2252A(a)(2)(A), and Section 2252A(a)(5)(B).

BACKGROUND OF THE INVESTIGATION

4. In the instant matter, a number of electronic service providers (ESPs) provided uploaded images of child pornography through CyberTipline Reports to the National Center for Missing & Exploited Children (NCMEC). ESPs are required by Title 18, United States Code, Section 2258A to report apparent child pornography to NCMEC through the CyberTipline when they become aware of said child pornography. Thereafter, NCMEC provided the content of the uploaded images to the New York State Police (NYSP) Internet Crimes Against Children (ICAC) Task Force of which HSI is a participating member. The NYSP ICAC thereafter provided the images of suspected child pornography to HSI.

5. An Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. Some computers have static or long term IP addresses while other computers have dynamic or frequently changing IP addresses. From my training and experience, I know that any computer that accesses the Internet must do so through an ISP. The ISP identifies the computer during the connection session by assigning it an IP address. This number is typically attached to all messages that come and go from the computer.

6. NCMEC is a non-governmental organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect that child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip. To make such a report, a company providing services on the internet, ESPs, can go to an online portal that NCMEC has set up for the submission of these tips. ESPs then can provide to NCMEC information concerning the child exploitation activity it believes to have occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. While ESPs will report the presence of any suspected child pornography they find to NCMEC, they do not conduct an exhaustive search of a user's e-mail account or cloud storage, but typically use some automated method for locating images of suspected child pornography. This may include the use of automated technologies that

compare the hash values of images contained in the user's account to the hash values of images of child pornography.

7. The ESP may also upload to NCMEC any files it collected in connection with the activity. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP or ESP provides, such as IP addresses. NCMEC then packages the information from the ISP and ESP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

8. In June of 2019, the Department of Homeland Security (DHS) HSI Special Agent in Charge (SAC) Buffalo, NY received a Cyber Tipline report from NCMEC via the New York State Police. This investigative lead was generated from NCMEC Cyber Tipline Reports # 44389559 and 44410467. These reports were submitted by Microsoft BingImage (Microsoft), regarding apparent child pornography. The incident time and date listed on the report is December 02, 2018 at 05:01:24 UTC and December 02, 2018 at 05:01:25 UTC. The reported user of the ISP account appears to be located in Hamburg, New York with the ISP as Verizon Fios.

9. The following information was also reported concerning the aforementioned NCMEC tip: the reported IP address: 108.17.54.54; Microsoft indicated on the NCMEC report that they became aware of the reported content which was uploaded in the BingImage infrastructure. Microsoft provided that (1) file was uploaded to the BingImage infrastructure

to include Filename: **8c9f0e48-7272-4f8b-9ac0-d002dae7580.jpg (File 1)** with assigned hash number: **MD5:84fe8c98ab778f94631a347272d85598**. According to the NCMEC report, the reporting ESP, Microsoft contemporaneously viewed the associated file, **(File 1)**. Microsoft categorized the file a content rating of B2, which is defined as "Pubescent Minor" and "Lascivious Exhibition." The categorization definition of "Lascivious Exhibition" created by ESP's in NCMEC CyberTip Reports is defined as: "Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value". On or about June 7, 2109, I viewed **(File 1)**. The image depicted the pubic area of a naked, prepubescent minor female. The genitalia of the minor female is being displayed in a lascivious manner thereby meeting the federal definition of child pornography.

10. I know from my training and experience that ESPs and ISPs flag and report images or files that have the same "hash values" as images that have been reviewed and identified by NCMEC or by law enforcement as child pornography. A hash value is akin to a fingerprint for a digital file. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value—the hash value—is produced that identifies the unique contents of the file. If the contents of a file are modified in any way, the hash value will change significantly. Even if only a single pixel in the image is modified (an alteration that would not likely be detected by the human eye), the hash value of the image will change. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

11. I also know from my training and experience that ISPs and ESPs compare the hash values of files that their customers transmit on their systems against a list of hash values known to be associated with files containing child pornography, which that NCMEC maintains. If the ISP or ESP finds that a hash value of a file on its system matches one on NCMEC's list, the ISP or ESP captures the file along with information about the user who posted, possessed, or transmitted it and submits that information to NCMEC as a CyberTip.

12. On or about February 7, 2019, ICAC Task Force law enforcement officers sent a DHS summons #2019-AY-1555 to Verizon Fios for subscriber information related to the IP address 108.17.54.54 for the date and time December 02, 2018 at 05:01:24 and 05:01:25 UTC as referenced in NCMEC Cyber Tipline Report 44389559 and 44410467.

13. On April 29, 2019 Verizon provided a response for the following subscriber information related to IP Address 108.17.54.54: Subscriber Name: David CALAIACOVO Subscriber Address: 4148 Wayfare Ct. Hamburg, NY 14075. Email address: starshipnxo1@yahoo.com Phone number: (716) 462-9724. Primary User ID: vze16y7fe and User Name: davec761.

14. On or about June 7, 2019, your affiant reviewed the following image file: **8c9f0e48-7272-4f8b-9ac0-d002dae7580.jpg (File 1)** , as previously mentioned, was obtained from the Microsoft NCMEC CyberTipline Reports # 44389559 and 44410467. The following is a description of the image:

> The picture is of one red haired pre-pubescent female child, approximately between the ages of 8 to 10 years old. The child is

> completely naked and only wearing a plaid in color necktie, sitting on the floor with her legs spread open, spread apart, exposing her genitals. The central focal point of the picture are undeveloped chest and genitals of the female child. The female child is in the middle of the picture with what appears to be in a classroom setting that includes a painted background of books on a shelf and a chalkboard. The photo also includes a globe, chair, desk, abacus and pencils on the floor with the child. No other individuals are depicted in this image.

15. Based on my training and experience, the above described image files meet the federal definition of child pornography, as defined in 18 U.S.C. § 2256(8), as they depict the lascivious exhibition of the genitals or pubic areas of a minor child.

16. Also in June of 2019, the DHS HSI Special Agent in Charge (SAC) Buffalo, NY received a (4) additional Cyber Tipline reports from NCMEC via the New York State Police. These investigative leads were generated from NCMEC Cyber Tipline Reports # 45855073, 45854993, 45855093 and 4583396. These reports were submitted by Microsoft BingImage (Microsoft), regarding apparent child pornography. The incident time and dates listed on the reports are all from January 19, 2019 at the times of 22:42:32, 22:55:33, 22:55:39 and 22:55:47 UTC. The reported user of the ISP account appears to be located in Hamburg, New York with the ISP as Verizon Fios.

17. The following information was also reported concerning the aforementioned NCMEC tips: the reported IP address: 108.17.54.54; Microsoft indicated on the NCMEC report that they became aware of the reported content which was uploaded in the BingImage infrastructure. Microsoft provided that (1) file was uploaded to the BingImage infrastructure to include Filenames: **c1e8f705-0ea9-404f-8bed-6ad0fe70b9a0.jpg, e2da5aa5-cf26-4681d2-**

a002082c9d09.jpg, b972557d-c964-428a-9bd4-15ec917fc948.jpg, 2476f-c4e9-4958-8f84ba7850f5.jpg (File 2) with assigned hash number: **MD5: 4459557a4b9a992d60a73af4849f3fb2**. According to the NCMEC report, the reporting ESP, Microsoft contemporaneously viewed the associated file, (File 2). Microsoft categorized the file a content rating of A2, which is defined as "Prepubescent Minor" and "Lascivious Exhibition." The categorization definition of "Lascivious Exhibition" created by ESP's in NCMEC CyberTip Reports is defined as: "Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value". On or about June 7, 2109, I viewed **(File 2)**. The image depicted the pubic area of a naked, prepubescent minor female. The genitalia of the minor female is being displayed in a lascivious manner thereby meeting the federal definition of child pornography.

18. On or about June 7, 2019, your affiant reviewed the following image file : **(File 2)** , as previously mentioned, obtained from the Microsoft NCMEC CyberTipline Reports # 45855073, 45854993, 45855093 and 4583396. The following is a description of the image:

> The picture is of one dark haired pre-pubescent female child, approximately between the ages of 4 to 6 years old. The child is completely naked, laying her side with one leg on the ground and the other leg is bent with her knee pointing up with her legs spread open, exposing her genitals. The central focal points of the picture are the undeveloped chest and genitals of the female child. The female child appears to be laying on sand near water. No other individuals are depicted in this image.

19. Based on my training and experience, the above described image files meet the federal definition of child pornography, as defined in 18 U.S.C. § 2256(8), as they depict the lascivious exhibition of the genitals or pubic areas of a minor child.

20. Also in June of 2019, the DHS HSI Special Agent in Charge (SAC) Buffalo, NY received an additional Cyber Tipline report from NCMEC via the New York State Police. This investigative lead was generated from NCMEC Cyber Tipline Report # 47172065. This report was submitted by Microsoft BingImage (Microsoft), regarding apparent child pornography. The incident time and dates listed on the report is from February 23, 2019 at the time of 22:45:29 UTC. The reported user of the ISP account appears to be located in Hamburg, New York with the ISP as Verizon Fios.

21. The following information was also reported concerning the aforementioned NCMEC tip # 47472065: the reported IP address: 108.17.54.54; Microsoft indicated on the NCMEC report that they became aware of the reported content which was uploaded in the BingImage infrastructure. Microsoft provided that (1) file was uploaded to the BingImage infrastructure to include Filename: **79f12a08-270d-4eed-8e75-4fec6b587b58.jpg (File 3)** with assigned hash number: **MD5: be40e29e86feda7aec74383d4bc0ebb6**. According to the NCMEC report, the reporting ESP, Microsoft contemporaneously viewed the associated file, (File 3). Microsoft categorized the file a content rating of A2, which is defined as "Prepubescent Minor" and "Lascivious Exhibition." The categorization definition of "Lascivious Exhibition" created by ESP's in NCMEC CyberTip Reports is defined as: "Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on

genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value". On or about June 7, 2109, I viewed **(File 3)**. The image depicted the pubic area of a naked, prepubescent minor female. The genitalia of the minor female is being displayed in a lascivious manner thereby meeting the federal definition of child pornography.

22. On or about June 7, 2019, your affiant reviewed the following image file **: (File 3)** , as previously mentioned, obtained from the Microsoft NCMEC CyberTipline Report # 47172065. The following is a description of the image:

> The picture is of one dark haired pre-pubescent female child, approximately between the ages of 4 to 6 years old. The child is completely naked, laying with her head and chest and knees are on the ground. The female child is positioned that her legs are spread exposing her undeveloped genital/anal region. The central focal point is the exposed undeveloped genital/anal region of the female child. The female child appears to be on the floor of a room, in front of a sofa or bed. No other individuals are depicted in this image.

23. Based on my training and experience, the above described image file meets the federal definition of child pornography, as defined in 18 U.S.C. § 2256(8), as they depict the lascivious exhibition of the genitals or pubic areas of a minor child.

SEARCH WARRANT AND SUBSEQUENT INVESTIGATION

24. On June 26, 2019, United States Magistrate Judge, H. Kenneth Schroeder for the Western District of New York approved a federal search warrant authorizing the search of CALAIACOVO's residence located at 4148 Wayfare Court Hamburg, NY 14075 (herein after SUBJECT PREMISES), which was executed on June 27, 2019 at approximately 06:00

a.m. During the execution of the search warrant, several items of evidence were located and seized, including a Toshiba Satellite L645D laptop computer with serial # YA053651W (**Line Item 004**), and numerous other electronic items to include a cell phones, an additional laptop computer, desktop computer towers, SD memory cards, Compact and Digital Video Discs (CD/DVD), VHS and Hi8 video tapes.

25. After entering and securing the SUBJECT PREMESIS, HSI Special Agent (SA) Kosich asked CALAIACOVO if he would speak privately outside the residence in HSI Group Supervisor (GS) James Kilpatrick's government-owned vehicle. At that time, SA Kosich told CALAIACOVO that Agents have a Search Warrant to his residence. CALAIACOVO stated that he would go to the vehicle and speak with agents. SA Kosich asked CALAIACOVO if he had any reason to believe why agents would be at his house. CALAIACOVO stated that he did not know. HSI GS Kilpatrick stated to CALAIACOVO that he was not under arrest and was free to leave at any time. CALAIACOVO was not restrained in any way during the interview.

26. During the non-custodial interview CALAIACOVO stated his internet service provider is Verizon Fios and has had service since he moved at the SUBJECT PREMESIS. CALAIACOVO stated that has worked in the school psychology field for the past 35 years and retired on Wednesday (June 26, 2019) from West Seneca Schools. CALAIACOVO also stated that his email address is starshipnxo1@yahoo.com. After about 22 minutes into the non-custodial interview CALAIACOVO stated that he was uncomfortable with answering

any more questions without representation. At that time, the questioning immediately stopped.

27. After the execution of the search warrant, the items seized including the Toshiba Satellite L645D laptop computer with serial # YA053651W (**Line Item 004**) found in Room "G" at the SUBJECT PREMESIS by HSI Special Agent James Donoghue, were transported to the HSI Buffalo Computer forensics lab for processing.

28. On July 1, 2019 HSI Computer Forensic Analyst (CFA) Henry Cameron conducted a preview of **Line Item 004** and opened File name "**Physical Sector 751116960-File Path: Partition 2 (Microsoft NFTS, 697.17 GB) TI105828W0G (Unallocated Clusters**). The following is a description of the image:

> The picture is a split image, the left side of the image is of one dark haired pre-pubescent female child, approximately between the ages of 4 to 5 years old. The child is only wearing yellow stockings and sitting on a bed with her legs spread apart exposing her undeveloped genitals and chest area. The child is looking at the camera with what appears to be a lollipop in her mouth. The right side of the image is a close- up of the vaginal/anal region of the female child. The central focal point of the right side of the image is the exposed undeveloped genital/anal region of the female child. No other individuals are depicted in this image.

29. Also on July 1, 2019 HSI (CFA) Cameron conducted a further preview of **Line Item 004** and opened File name "**Physical Sector 72864664-File Path: Partition 2 (Microsoft NFTS, 697.17 GB) TI105828W0G (Unallocated Clusters**). The following is a description of the image:

> The picture is of one dark haired pre-pubescent female child, approximately between the ages of 3 to 5 years old. The child is completely naked, laying on her chest with her knees on the ground with

her face looking back at the camera. The female child is on yellow in color floral patterned blanket. The female child is positioned that her hands are used to spread apart her buttocks exposing her undeveloped genital/anal region. The central focal point is the exposed undeveloped genital/anal region of the female child. No other individuals are depicted in this image.

30. Also on July 1, 2019 HSI (CFA) Cameron conducted a further preview of **Line Item 004** and opened File name "**{0645cc3c-32f0-11e9-9897-c80aa9f1f9c7}{3808876b-c176-4e48-b7ae-04046e6cc752} File Path: Partition 2 (Microsoft NTFS, 697.17 GB) TI105828W0G\System Volume Information**. The following is a description of the image:

> The picture is of a pre-pubescent female child, approximately between the ages of 3 to 5 years old. The child is wearing both a pink shirt and a white undershirt. The female child is naked from the waist down, with her hands on the backs of her legs spreading apart and exposing the undeveloped vaginal region of the female child. There appears to be a clear glass or plastic dildo inserted in the female child's anus. The female child appears to be sitting on a green in color pillow, with a plastic cover. The central focal point of the image is the exposed undeveloped genital region of the female child, and the insertion of the clear dildo in the anus. No other individuals are depicted in this image.

31. Also on July 1, 2019 HSI (CFA) Cameron conducted a further preview of **Line Item 004** and opened File name "**{dd4f7e76-5b34-11e9-8a14-c80aa9f1f9c7}{3808876b-c176-4e48-b7ae-04046e6cc752} File Path: Partition 2 (Microsoft NTFS, 697.17 GB) TI105828W0G\System Volume Information**. The following is a description of the image:

> The picture is of a pubescent female child, approximately between the ages of 10 to 12 years old. The child is completely naked but is wearing sandals on her feet. The female child is squatting down in a field, facing the camera with her left hand on the ground and her right hand is in front of her. The female child is looking at the camera, with her legs spread open, exposing the undeveloped genital and chest region of the female child. The central focal point of the image is the exposed undeveloped genital region and chest of the female child. The logo "LS Island" appears in the upper left-hand corner of the image. No other individuals are depicted in this image.

32. Also on July 1, 2019 HSI (CFA) Cameron conducted a further preview of **Line Item 004** and opened File name **": Physical Sector 74558448 File Path: Partition 2 (Microsoft NTFS, 697.17 GB) TI105828W0G (Unallocated Clusters)** The following is a description of the image:

> The picture is of a pre-pubescent female child, approximately between the ages of 4 to 6 years old with an adult male. The adult male is naked, laying on a green in color blanket on his back with his legs spread open exposing his erect penis. The child is completely naked laying on her stomach in between the legs of the adult male and her mouth is on the anal region of the adult male. The central focal point of the image is the exposed male and face of the pre-pubescent in the anal region of the adult male. No other individuals are depicted in this image.

CONCLUSION

33. Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe **David Michael CALAIACOVO**, has violated Title 18, Title 18, United States Code, Section 2252 2252A(a)(2)(A) [Receipt of Child Pornography], and 2252A(a)(5)(B) [Possession of Child Pornography].

JOHN A. KOSICH, JR.
Special Agent
Homeland Security Investigations

Sworn to and subscribed before
me this 2nd day of July, 2019.

MICHAEL J. ROEMER
United States Magistrate Judge